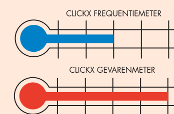
Hoe gevaarlijk is internet, en wat doe je er

De gruwelen van het

Horrorfilms stellen niks meer voor als je al die griezelverhalen mag geloven die de ronde doen over het internet! Hackers, spammers, virussen en spyware… het wemelt blijkbaar van duistere figuren en verdachte programma's die het op jou gemunt hebben. Hoe gevaarlijk is internet eigenlijk, en op welke manier kan je je ertegen wapenen? Clickx ging het voor jou na.

De fun is eruit, lijkt de boodschap van de media, het net stikt van de cybercriminelen. Heb je geen diploma computerbeveiliging op zak, dan mag je het wel schudden: jouw pc binnendringen is een peulenschil… Clickx is gelukkig iets genuanceerder: je kan echt niet buiten enige bescherming, maar met enkele voorzorgsmaatregelen én wat gezond verstand is het op het net best leuk – én veilig – vertoeven! Met welke bedreigingen je precies hebt af te rekenen, kom je in dit artikel te weten. Aan de hand van onze frequentiemeter lees je ook af hoeveel kans je loopt dat je er zonder extra beveiligingen mee in aanraking komt, en onze gevarenmeter vertelt je hoe link die ondingen nu echt wel zijn. En Clickx zou Clickx niet zijn als we je er meteen ook niet bij vertelden hoe je die gevaren kan afweren, en wat je best wél en niét doet. Het aantal duimpjes maakt je meteen diets hoe efficiënt die remedie wel is!

Hackers



Gezellig een potje surfen lijkt toch niet zo'n ongevaarlijke bezigheid, als je sommige sites mag geloven. Kijk maar even naar de afbeelding: zo'n bericht krijg je prompt op je neus zodra je die site nog maar binnenwandelt. Het lijkt wel alsof allerlei instanties heimelijk al je internetverkeer monitoren… Zo'n vaart loopt het gelukkig niet: je moet namelijk weten dat deze site privacy-software tracht te slijten en via een bericht als dit vooral de angst van de surfer tracht aan te wakkeren. Feit blijft natuurlijk dat ze blijkbaar moeiteloos weten uit te vissen via welke provider je surft. Dat klopt, maar daar hoef je je echt niet zoveel zorgen om te maken. Bij elke internetconnectie krijgt je pc van je provider namelijk een IP-adres toegewezen. Dit adres (dat uit vier cijfers tussen 0 en 255 bestaat) stuurt je pc vervolgens

449 TELENET Investigation

Your computer has been tracked.

Your IP is under investigation:	*213.224.94.160*
Your ISP is co-operating:	*TELENET*
They know you are using:	*Microsoft Internet Explorer v6*
Your computer is:	*Windows XP*
Your risk status for further investigation:	*VERY HIGH RISK*

Your computer is full of evidence. You need help now.

Years of Internet data could be used by the police.

Www.evidence-eliminator.com: is Big Bother watching yuo?

aan?
net



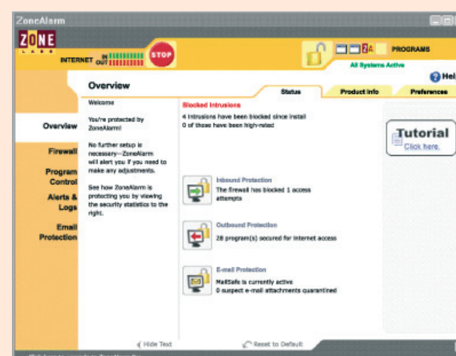
door naar elke internetcomputer waarmee je verbinding zoekt. Dat is nodig opdat die computer zou weten waar hij zijn reactie naartoe moet sturen. Surf je bijvoorbeeld naar een website, dan krijgt ook die computer jouw IP-adres te zien, en na enig opzoekwerk kan die je prompt meedelen wie je provider is. Even schrikken dus, dat wel, maar al bij al best onschuldig.

Open de poort

Wat nu als een hacker ofte computerinbreker jouw IP-adres te pakken krijgt? Dat is nauwelijks erger dan wanneer een 'klassieke' inbreker je fysieke adres uitvist: hij weet dan wel je woning staan, maar als je alle poortjes goed gesloten houdt, hoef je niet veel te vrezen. Wat veel surfers echter niet weten, is dat ook hun pc over heel wat (genummerde) poortjes beschikt, een paar tienduizenden zelfs! Standaard opent je browser bijvoorbeeld poort 80 om je te laten surfen. Tik maar even het adres [**http://www.clickxmagazine.be:80**] in (in plaats van [**http://www.clickxmagazine.be**]): je zal merken dat je hetzelfde resultaat krijgt, terwijl je met een ander poortnummer bot vangt.
Het probleem is nu dat een modale computergebruiker moeilijk zicht krijgt op welke poorten (al dan niet horen) geopend (te) zijn. Gelukkig bestaat er speciale software die al het verkeer dat van en naar je pc gaat monitort. Zulke software noemen we een firewall, en je kan de functie een beetje vergelijken met een grenswachter: geldig (en onschuldig) verkeer geraakt erdoor, de rest wordt tegengehouden. Een van de populairste firewalls is ongetwijfeld ZoneAlarm [**www.zonelabs.com**] die je bovendien in een gratis versie kan downloaden. Zo'n firewall vergt vooral in het begin wel enig configuratiewerk, maar ZoneAlarm komt je daarbij een heel eind tegemoet en kan bijvoorbeeld het verkeer van betrouwbare software zoals je browser of e-mailprogramma vrijelijk doorlaten. Wil ook andere software het net op, dan krijg je een alarmberichtje te zien waarna je zelf moet beslissen of je dat verkeer toelaat of niet.

Gaatjes

Met zo'n firewall spijker je dus al heel wat ongewenste toegangen toe, maar jammer genoeg is Windows zelf ook niet waterdicht, en zijn hackers altijd op zoek naar gaatjes in het besturingssysteem die ze vervolgens kunnen misbruiken (exploits). Om die reden brengt Microsoft om de haverklap zogenaamde patches uit: software die dergelijke gaatjes hoort te dichten. Wil je dus veilig(er) het net op, dan kan je niet buiten een regelmatige update van Windows! Microsoft maakt het je overigens wel makkelijk om zulke updates uit te voeren. Afhankelijk van je Windows-versie en instellingen kan dat zelfs zo goed als volautomatisch gebeuren. In Windows XP bijvoorbeeld klik je daarvoor **Deze computer** met de rechtermuistoets aan, kies je **Eigenschappen** uit het snelmenu, en open je het tabblad **Automatische updates**. Je kan overigens ook altijd zelf naar [**http://windowsupdate.microsoft.com**] surfen. Updates en patches voor Microsoft Office vind je op [**http://office.microsoft.com/officeupdate**].

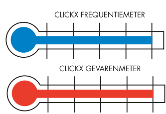


ZoneAlarm: een gratis firewall voor thuisgebruikers.

DOEN

✔ Een firewall installeren en configureren
✔ Geregeld updates van Windows (en Office) downloaden en installeren

Virussen, wormen, Trojaanse paarden en… hoaxes..



Misschien heb je onlangs wel een e-mailbericht van Microsoft ontvangen, met als bijlage precies zo'n patch die je dringend hoorde te installeren. Erg vriendelijk natuurlijk, ware het niet dat de e-mail niet van Microsoft afkomstig was en dat die bijlage… een virus bevatte (het Swen-virus)! Virussen zijn eigenlijk weinig meer dan programmaatjes die zichzelf vermenigvuldigen – door bijvoorbeeld andere bestanden met een kopie van zichzelf te infecteren – en die heel vaak venijnige foefjes met je systeem uithalen. Nauw verwant hieraan zijn de zogenaamde wormen, die zich gewoonlijk via e-mail razendsnel over het internet weten te verspreiden. Meestal komt zo'n worm vermomd als een onschuldige bijlage, en eens je die opent stuurt de worm een kopie van zichzelf naar bijvoorbeeld alle adressen uit je adresboek. Je kan je voorstellen dat zo'n razendsnelle worm heel wat mailservers erg zwaar belast, zodat sommige zelfs onder het gewicht van al het bijkomende verkeer bezwijken. In sommige wormen schuilt zelfs nog wat meer venijn: ze kunnen namelijk ook een heuse viruscomponent bevatten die ook je eigen pc op een of andere manier schade kan berokkenen.

Ten slotte zijn er nog de Trojaanse paarden. Het lijkt dan wel om een nuttig programmaatje te gaan – en mogelijk doet het ook zinvolle dingen – maar jammer genoeg bevat het in 't geniep ook een verderfelijke module. Zo'n Trojaans paard zal bijvoorbeeld heimelijk persoonlijke gegevens uit je pc via je internetverbinding doorsluizen, of het kan een nuttig wapen zijn in handen van een hacker die daarmee vanop afstand jouw computer kan besturen en er allerlei fratsen mee uithalen – zoals een aanval lanceren op een of andere bekende site… en met jouw IP-adres! Het aantal virusachtige ondingen wordt momenteel geschat op zo'n 80.000, maar dagelijks groeit hun aantal nog aan. Wil je hierover meer informatie, dan kan je een on line virusencyclopedie raadplegen, zoals die op [**www.avp.ch/avpve**] of [**www.trendmicro.com/vinfo/virusencyclo**].

Pas op je tellen

Wie tussen de regels door heeft gelezen, begrijpt dat heel wat van dit ongedierte je pc bereikt via e-mail, gewoonlijk verstopt in bijlagen. Voorzichtig omspringen met e-mails (van onbekenden) is dus een eerste vereiste! Zelfs als het om een onschuldig .doc of .ppt-document lijkt te gaan, moet je op je tellen passen. In zo'n Word-document huist misschien een zogenaamd macrovirus, en bovendien kan een onschuldig ogend bestand altijd nog een verborgen extensie bevatten, (.ppt.scr of .jpg.exe bijvoorbeeld). Hoe dan ook, je kan echt niet buiten een antivirusprogramma – dat je bovendien heel frequent moet updaten! Een sporadische viruscheck on line is altijd wel mogelijk (gratis op onder meer: [**http://housecall.antivirus.com**] en [**www.ravantivirus.com/scan**]), maar uiteindelijk toch ontoereikend. Wil je het euh… kost wat kost gratis houden, dan kan je voor de installatie van een heus antivirusprogramma hier aankloppen: [**www.avast.com**] en [**www.free-av.com**]. Commerciële antiviruspakketten zijn er natuurlijk ook, en dat van Norton komt in heel wat onafhankelijke tests geregeld als beste uit de bus [**www.symantec.com**]. Net zoals bij vele andere pakketten, kan je Norton Antivirus ook zo instellen dat updates automatisch worden uitgevoerd via het net.

Hoaxes

Virussen zijn dus best wel kwalijke beestjes, maar anderzijds mag je je ook niet in de luren laten leggen door zogenaamde hoaxes. Dat zijn e-mails waarin je gewaarschuwd wordt voor een of ander nieuw supervirus dat wellicht al je pc is binnengedrongen. Heel vaak wordt je dan meteen gevraagd een of ander bestand op je pc te wissen. De kans is echter groot dat het om een vals bericht gaat, en dat het gewraakte bestand (zoals sulfnbk.exe of jdbgmgr.exe) hoegenaamd niet van het vermeende virus afkomstig was! Twijfel je of het om een hoax gaat, dan kan je nog altijd te rade gaan bij [**www.vmyths.com**].

Van: MS Corporation Customer Assistance **Aan:** Microsoft Client
Onderwerp: Latest Microsoft Security Upgrade

Microsoft All Products | Support | Search | Microsoft.com Guide
Microsoft Home



MS Client

this is the latest version of security update, the "October 2003, Cumulative Patch" update which resolves all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three newly discovered vulnerabilities. Install now to protect your computer from these vulnerabilities, the most serious of which could allow an malicious user to run executable on your system. This update includes the functionality of all previously released patches.

System requirements	Windows 95/98/Me/2000/NT/XP
This update applies to	MS Internet Explorer, version 4.01 and later MS Outlook, version 8.00 and later MS Outlook Express, version 4.01 and later
Recommendation	Customers should install the patch at the earliest opportunity.
How to install	Run attached file. Choose Yes on displayed dialog box.
How to use	You don't need to do anything after installing this item.

Microsoft Product Support Services and Knowledge Base articles can be found on the Microsoft Technical Support web site. For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site, or Contact Us.

Microsoft, met een Swen-reukje aan.

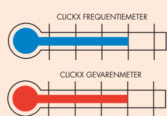
DOEN

- ✔ Een anti-virusprogramma installeren en up-to-date houden
- ✔ Alle inkomende én uitgaande e-mails op virussen laten checken

NIET DOEN

- ✘ Zomaar e-mailberichten - met bijlagen - van onbekenden openen
- ✘ E-mail met (valse) virusberichten naar je kennissen doorsturen

Spyware



Met spionnen hebben brave burgers als jij en ik natuurlijk niks te maken, maar de kans bestaat dat er zich een paar exemplaren... in je pc genesteld hebben. Het gaat natuurlijk alweer om programmaatjes die je er wellicht zelf op hebt geïnstalleerd, zonder dat je je van enig kwaad bewust was. De meest onschuldige vorm van dergelijke 'spyware' (pests) is de zogenaamde adware. Dat is software die heimelijk van je internetconnectie gebruik maakt om af en toe nieuwe advertenties van een of andere webstek binnen te halen en op je scherm te ploffen. Heel vaak vormt adware een onderdeel van allerlei tools die je kan downloaden. Die tools zijn dan wel gratis, maar je 'betaalt' in de vorm van advertenties. Sommige vormen van spyware zijn echter venijniger, en sturen bijvoorbeeld geregeld informatie over je surfgedrag naar hun makers door.

Bekende tools die van allerlei spyware vergezeld gaan, zijn Kazaa en Grokster. Wil je meer weten over welke spyware er zoal bestaat en wat die precies met je pc uitvreet, dan kan je [**www.spywareguide.com**] raadplegen. Die bevat een lijst met zo'n 300 verschillende spyware-tools. We raden je ook aan af en toe je systeem met een spionnenjager door te lichten. Dat hoeft je trouwens geen eurocent te kosten, want de anti-spyware programma's Ad-aware [**www.lavasoftusa.com**] en SpyBot Search & Destroy [**www.safer-networking.org**] doen niet alleen prima hun werk, ze zijn ook geheel gratis! Verkies je een on line check-up, dan kan je terecht op [**www.pestscan.com**] (enkel scannen, niet verwijderen).



Dit systeem lijkt wel erg grondig ver-pest.

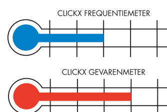
DOEN

✔ Je systeem sporadisch checken met een anti-spywareprogramma

NIET DOEN

✘ Zomaar (gratis) tools downloaden zonder de voorwaarden na te gaan

Dialers en browser hijackers



Wij hebben het natuurlijk ook maar van horen zeggen, maar vooral bij pornografische sites is het uitkijken geblazen – en zeker wanneer je met een analoge modem en een gewone telefoonlijn het net opgaat... Niet zelden verschijnt op zo'n site namelijk het aanlokkelijke bericht dat je een of ander gratis tooltje kan downloaden zodat je nog sneller van al die fraaie beelden kan genieten. Dus, even sponzen maar, dat ding? Beter niet, want de kans is groot dat het om een zogenaamde dialer gaat. Dat is een programmaatje dat tersluiks de gegevens van je inbelverbinding aanpast, zodat je in het vervolg niet langer je provider opbelt, maar wel een van hun eigen diensten op een of andere exotisch eiland, waar je voor elke minuut internetverbinding ettelijke euro's aan je telecomoperator mag afdragen!

Beveiligingswaarschuwing

Wilt u Hot Adult Download! Click YES below installeren en uitvoeren, getekend op 21/05/2002 22:19 en gedistribueerd door:

De authenticiteit van de uitgever is door VeriSign Class 3 Code Signing 2001-4 CA gecontroleerd.

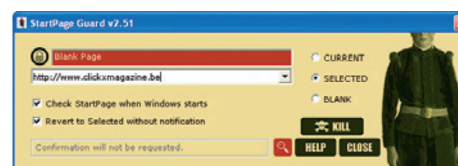
Let op: beschouwt deze inhoud als veilig. Ga alleen verder als u erop vertrouwt dat Proclaim Telcom, Inc. dit kan bepalen.

☐ Inhoud van altijd vertrouwen

Ja | Nee | Meer info

Even inbellen naar de provider in euh... Tuvalu?

Louche sitebeheerders hebben overigens nog wel meer in hun mouw steken. Zo heb je voor je het goed en wel beseft hun site tot startpagina van je browser gebombardeerd, en wat je nadien ook onderneemt: je krijgt die pagina daar met geen stokken meer weg! Zulke trucjes kennen we onder de naam 'browser hijacker' (browserkaper). Hiervoor bestaan wel een paar specifieke oplossingen (waaronder StartPage Guard, [**http://pjwalczak.com/spguard/index.php**]) een gratis tool die zo'n kaping verhindert), maar met de bovenvermelde anti-spywaretools kan je de meeste dialers en hijackers ook wel te grazen nemen. Met wat geluk kan je het onding ook wel manueel verwijderen (via het CONFIGURATIESCHERM, SOFTWARE, of via de opdracht MSCONFIG waar je de vinkjes verwijdert naast verdachte programma's op het tabblad OPSTARTEN), maar dikwijls volstaat zo'n ingreep niet.

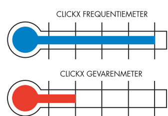


Een schildwacht voor je startpagina.

NIET DOEN

✘ Zomaar programmaatjes (in pop-upvensters) vanop een website laten uitvoeren

POP-UPS



Sommige websites – zoals pornosites – doen enorm veel moeite om de bezoeker bij zich te houden. Telkens je hun stek wil verlaten, duiken namelijk een hele rist vensters op die zich ofwel bovenop het huidige browservenster (pop-ups) ofwel stiekem onder dat venster (pop-unders) nestelen. Wie bijvoorbeeld [**www.porn.com**] durft te bezoeken, weet onmiddellijk hoe laat het is! Knap vervelend dus, maar gelukkig kan je met de juiste software ook hier wel een stokje voorsteken. Daar bestaan natuurlijk ook commerciële tools voor, maar wij wisten alvast enkele degelijke, gratis anti-pop-up tools op de kop te tikken: Pop-Up Stopper Free [**www.panicware.com**] en STOPzilla [**www.stopzilla.com**].

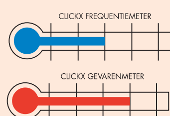


Pop-Up Stopper aan het werk.

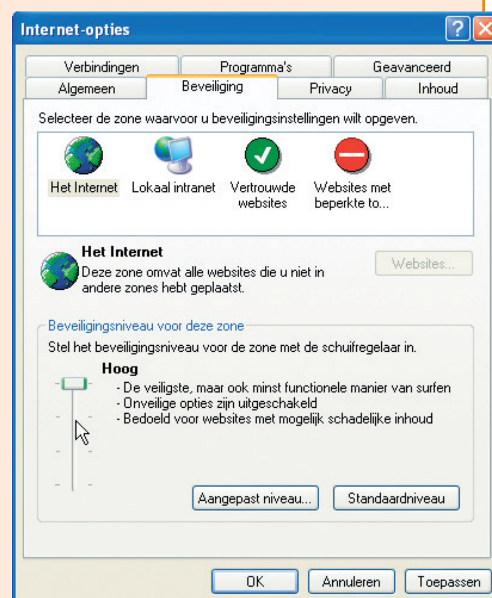
DOEN

✔ Een pop-up blocker installeren 

SCRIPTS



Heel wat geniepiger – en gevaarlijker – dan pop-ups zijn kwaadaardige scripts. Een script is een klein programmaatje (Java, ActiveX) dat aan een of andere webpagina is gekoppeld en dat allerlei onheil op je pc kan uitrichten, zoals het wissen van bestanden of het installeren van spyware. Je hoeft nu niet onmiddellijk een surffobie te ontwikkelen, want dergelijke scripts maken vooral kans als je met een niet up-to-date browser zit opgescheept én je de browserbeveiliging te laks hebt ingesteld. Ook hier is het dus erg belangrijk dat je (via de Windows updatesite) frequent patches voor je browser installeert. Je hoeft ook helemaal geen expert te zijn om een browser als Internet Explorer veilig af te stellen. Daarvoor moet je in het menu EXTRA zijn, waar je INTERNET-OPTIES selecteert. Open vervolgens het tabblad BEVEILIGING, kies de zone INTERNET en verschuif het beveiligingsniveau voor deze zone minstens naar NORMAAL. Nog een trapje hoger geeft je natuurlijk wel dat ietsje meer veiligheid, maar de kans bestaat dat dan ook bepaalde goedaardige webpagina's niet langer perfect binnenrollen. Ben je wat beslagen in browserterminologie, dan kan je het beveiligingsniveau echter ook exact naar wens afstemmen via de knop AANGEPAST NIVEAU.
Wat extra beveiliging inbouwen kan natuurlijk nooit kwaad, en dat is precies hoe Spyware Blaster [**www.javacoolsoftware.com/spywareblaster.html**] erover denkt. Deze tool voorkomt dat spyware zich via ActiveX-controls vanop webpagina's kan installeren. Een ingebouwde update-optie zorgt ervoor dat ook nieuwe vormen van spyware geen kans krijgen...

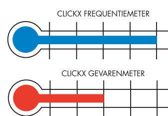


Geef je browser niet té veel speelruimte.

DOEN

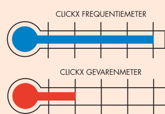
✔ Geregeld up-to-date patches voor je browser installeren
✔ De beveiligingen van je browser voldoende hoog instellen
✔ Een script-checker installeren 

COOKIES



Bij het woord 'cookies' hoef je niet onmiddellijk naar je koekjestrommel te hollen. Cookies zijn namelijk niks anders dan kleine bestandjes die zich tijdens het surfen op je harde schijf kunnen nestelen. Op zich onschuldige tekstbestandjes, die erop gericht zijn je surfcomfort te verhogen. Dankzij zo'n cookie kan een site bijvoorbeeld onthouden welke taal je verkiest, of welke pagina's je bij een vorig bezoek hebt bekeken, of welk wachtwoord je voor de site-toegang gebruikt. Veel zorgen hoef je je daar niet om te maken, want websites kunnen in principe enkel hun eigen cookies inlezen. Toch is ook hier enige voorzichtigheid geboden, met name als het om 'tracking cookies' gaat die je surfgedrag in kaart trachten te brengen. Het volgende scenario bijvoorbeeld is heel typisch. Een on line advertentiebureau plaatst met medeweten van de sitebeheerders zogenaamde 'webbugs' – onzichtbare afbeeldingen (1 x 1 pixel) – op diverse pagina's in tal van websites. Bezoek je nu één van deze pagina's, dan kan dat bureau heimelijk een cookie op je schijf plaatsen, met daarin de pagina je net hebt bezocht. Dat gebeurt telkens je een webstek bezoekt die zo'n webbug bevat. Zo krijgen ze een goed idee van je surfgedrag, en kan men je bijvoorbeeld heel gerichte banneradvertenties of pop-ups laten zien wanneer je een van de bewuste pagina's bezoekt. Ben je dit onzichtbare ongedierte liever kwijt dan rijk, dan kan je op [**www.bugnosis.org**] terecht voor een gratis tool waarmee je webbugs niet alleen zichtbaar kan maken, maar ze meteen ook verdelgt.
Ook Internet Explorer zelf helpt je een gezond cookiebeheer uit te bouwen. Daarvoor moet je opnieuw bij INTERNET-OPTIES in het menu EXTRA zijn, maar dit keer open je het

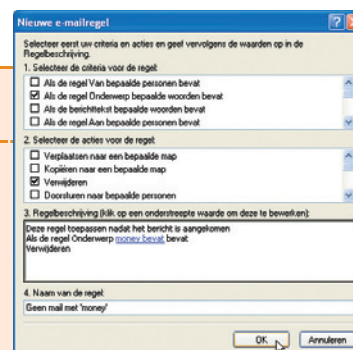
Spam



Op zich niet gevaarlijk, maar wel een echte pest zijn de zogenaamde spamberichten: doorgaans commercieel getinte e-mailberichtjes waar je zelf niet om gevraagd hebt en die vaak naar tienduizenden ontvangers tegelijk worden verstuurd. Daar bestaat wel nationale en Europese wetgeving rond, maar dat brengt natuurlijk weinig zoden aan de dijk als de meeste spam vanuit het buitenland – en vooral dan de VS – vertrekt… Gelukkig zijn er wel een aantal strategieën waarmee je de stortvloed aan spam wat kan indijken. Een boze reply naar de spammer sturen is alvast geen goed idee want heel wat berichten maken gebruik van ‘e-mail spoofing’, waarbij het afzendadres vervalst is. Nog minder verstandig is ingaan op de vraag of je voortaan liever geen e-mails meer van deze verzender ontvangt. Doe je dat toch, dan weet de spammer dat je e-mailadres actief is en mag je je aan nog meer van dergelijke berichtjes verwachten. Wat kan je dan wél doen? Om te beginnen je (echte) e-mailadres niet zomaar rondstrooien. Moet je toch een e-mailadres invullen op een ‘verdachte’ site, gebruik dan een tijdelijk webadres (genre Hotmail) of vraag een gratis wegwerpadres aan op een site als [**www.spammotel.com**]. Ontvang je inderdaad spam op dat adres, dan kan je het heel makkelijk weer verwijderen.
Een alternatieve strategie – die ook geschikt is om virussen via e-mail tegen te gaan – is de installatie van een zogenaamde ‘pre-deleter’. Dat is een tool die net als je e-mailprogramma je mailbox leegt, maar in eerste instantie enkel de afzender, onderwerp en grootte van het bericht toont. In deze fase beslis je dan of je het bericht effectief wil laten binnenkomen of al meteen op de mailserver wil laten wissen. MailWasher is zo’n gratis tool [**www.mailwasher.net**], overigens met een leuk extraatje: je kan een mailtje ook laten ‘bouncen’ (terugbotsen) naar de afzender, zodat het lijkt alsof je e-mailadres ongeldig is. Ook Outlook (Express) heeft een soort anti-spammodule ingebouwd. Je kan namelijk binnenkomende berichtjes op bepaalde kernwoorden filteren. Zo is het perfect mogelijk alle berichtjes die het word ‘money’ bevatten, automatisch in de map met Verwijderde items te deponeren. In Outlook Express doe je dat als volgt: kies in het menu **Extra** voor **Berichtregels** en vervolgens **E-mail**. Druk nu op de knop **Nieuw**, en duid de gewenste criteria aan. Vind je deze ingebouwde filtervoorziening iets te zwak, dan kan je nog altijd je toevlucht nemen tot een extern hulpprogramma met nog meer anti-spam pijlen op z’n boog. Een van de beste is SpamKiller [**www.spamkiller.com**], maar dat kost je dan wel 39,95 USD. Een bruikbaar, maar gratis alternatief is SpamAssassin [**www.spamassassin.org**].

Messenger

Vrij nieuw zijn de zogenaamde Messenger-spams. Wees gerust, die hebben niks te maken met de populaire MSN – of Windows Messenger, maar wel alles met een netwerkservice die standaard in Windows XP is geactiveerd. Spammers misbruiken deze service en slagen er op die manier in pop-upvenstertjes op je scherm neer te zetten. Om dat te vermijden kan je die service manueel uitschakelen via je Configuratiescherm, maar het kan nog makkelijker met behulp van een gratis tooltje (Shoot the Messenger) waarmee je de service naar eigen keuze snel kan in- en uitschakelen [**www.grc.com/stm/ShootTheMessenger.com**].



Ongewenste mail snel even uitfilteren.

DOEN

- ✔ Anti-spam filter activeren in Outlook (Express)
- ✔ Een tijdelijk (wegwerp)adres gebruiken
- ✔ Pre-deleter en/of anti-spamtool installeren
- ✔ Windows Messenger service uitschakelen

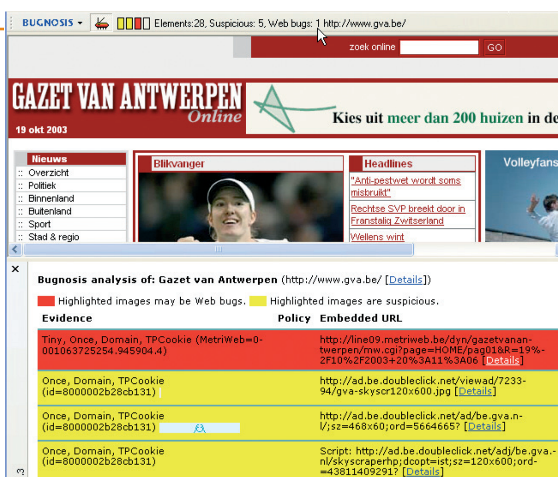
NIET DOEN

- ✘ Je e-mailadres rondstrooien
- ✘ Zelf reageren naar de verzender van een spambericht

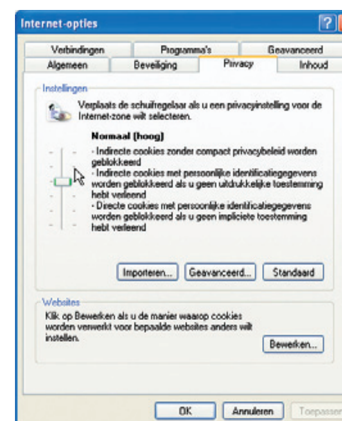
tabblad **Privacy**. Zet je de schuifbalk op **Normaal (hoog)** of **Hoog**, dan maak je het leven van dergelijke traceer-cookies al behoorlijk lastig. Via de knop **Geavanceerd** en **Bewerken** kan je echter nog specifiekere Cookie-instellingen kwijt.

DOEN

- ✔ Het cookiebeleid van je browser voldoende hoog instellen
- ✔ Een webbug-detector installeren

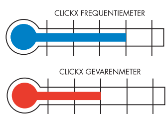


Bugnosis: allemaal beestjes…

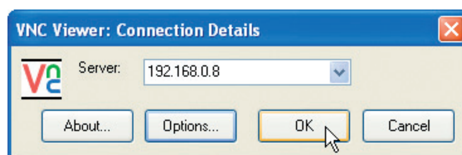


Internet Explorer: goede cookiebeheerder aan boord.

Aanstootgevende inhoud



We hoeven het je al niet meer te vertellen: het internet is een schitterende bron van informatie, maar er zit ook veel kaf tussen het koren. Zo kan heel wat inhoud – op nieuwsgroepen en in websites – erg aanstootgevend zijn, en bijvoorbeeld expliciet gewelddadig of pornografisch materiaal bevatten. Natuurlijk had je je kinderen daartegen graag afgeschermd. Geen eenvoudige opgave, want dergelijk materiaal duikt niet zelden ongewild op, bijvoorbeeld tijdens een zoektocht naar wat leuke, gratis software... De meest geschikte pedagogische aanpak laten we het liefst aan anderen over, maar over de technische mogelijkheden spreken we ons wel graag uit. Een mogelijke aanpak is de installatie van een programma waarmee je vanop afstand alles kan volgen – en zelfs beheren – wat op een andere computer gebeurt.



Stiekem meegluren vanop een andere pc.

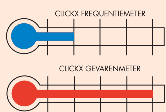
Dat veronderstelt echter wel dat beide computers hetzij in een netwerkje hangen, hetzij beide rechtstreeks met het internet verbonden zijn. Helemaal gratis en al bij al niet zo moeilijk in gebruik is RealVNC [**www.realvnc.com**].

Je kan ook een filterprogramma installeren waarmee je de toegang tot het internet niet alleen qua tijd (bijvoorbeeld: enkel surfen tussen 18 en 19 uur) maar ook qua ruimte kan beperken. Dat laatste gebeurt vaak aan de hand van een ingebouwde filterset die automatisch de toegang tot (bekende) pornosites e.d. verbiedt. Uiteraard kan je ook eigen sites aan die lijst toevoegen. De betere programma's zorgen voor automatische updates van die filterset, maar garanties dat er geen 'verkeerde dingen' doorsijpelen, heb je nooit! Eén van de bekendste en betere tools is CyberPatrol ([**www.cyberpatrol.com**], € 39), maar er is ook een gratis oplossing die behoorlijk functioneert: iProtectYou Free ([**www.softforyou.com/ip-free.html**] – op deze stek vind je ook een pdf-bestand met tal van tips om je kinderen on line te beschermen).

DOEN

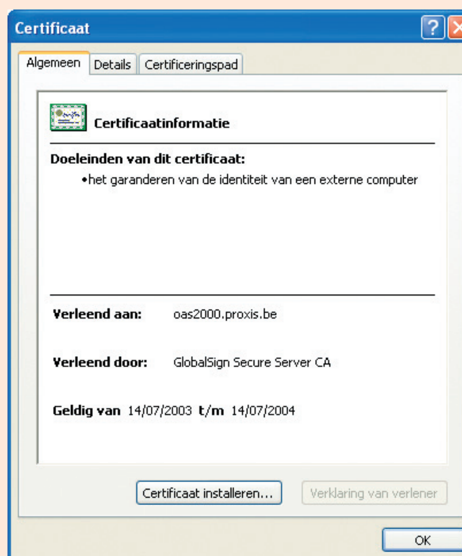
- ✔ Software voor afstandsbediening en -monitoring installeren
- ✔ Een kindvriendelijke filter installeren

On line fraude



Heel wat spookverhalen doen de ronde over on line fraude: je bestelt iets on line, maar de bestelling komt gebrekkig of helemaal niet aan, en je bent je lieve centjes kwijt. Of nog: je kredietkaartgegevens zijn via het net in verkeerde handen terechtgekomen, en er is blijkbaar geld opgenomen... Misbruiken zijn er natuurlijk altijd – net als in de 'echte' wereld – maar als je een beetje uitkijkt, kan je al veel leed voorkomen. Een vuistregel bij on line betalen is alvast dat je nooit je persoonlijke gegevens intikt op een niet-beveiligde webpagina, aangezien in dat geval je gegevens in leesbare vorm over het net worden versast. Enkel als de pagina een adres heeft dat met https:// begint (s staat voor secure) én je browser onderaan een gesloten hangslotje toont, kan je veilig je gegevens kwijt. Meer informatie over de beveiliging krijg je overigens na een dubbelklik op dat hangslotje. Voorwaarde voor een veilige transactie blijft natuurlijk wel dat de verkoper een betrouwbare instantie is. Dat kan je niet altijd makkelijk nagaan, maar in principe betalen kredietkaartmaatschappijen je aankoop wel terug als blijkt dat het om een malafide handelaar gaat.

Tot slot, heb je kinderen in huis, dan doe je er goed aan een bijkomende beveiliging te installeren die voorkomt dat persoonlijke gegevens (adres, kredietkaartnummers, wachtwoorden, ...) je pc verlaten. Zo'n functie tref je onder meer aan in de Internet Security pakketten van Norton en McAfee ([**www.symantec.com**], 69,95 USD en [**www.mcafee.com**], 69,99 USD). Met deze all-rounders haal je overigens zowat alle mogelijke modules in huis voor een stevige protectie: antivirus, anti-spam, anti-spyware, firewall, privacy bewaker, kindvriendelijke filter, popup blokker, enz...



Een gesloten hangslotje: veilig(er) betalen.

DOEN

- ✔ Een privacy-bewaker installeren

NIET DOEN

- ✘ On line betalen via een niet-beveiligde webpagina

— Toon Van Daele —